John J. Nelson (SBN 317598)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN PLLC
401 W. Broadway, Suite 1760
San Diego, CA 92101
Tel: (858) 209-6941
jnelson@milberg.com

Attorney for Plaintiff

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

JOSEPHINE DIBISCEGLIA, on behalf of herself and all others similarly situated, Plaintiff, vs. **ETHOS TECHNOLOGIES, INC.,** Defendant.	Case No.: _____ **CLASS ACTION COMPLAINT** DEMAND FOR JURY TRIAL

Plaintiff Josephine Dibisceglia, individually, and on behalf of all others similarly situated, brings this Class Action Complaint ("Complaint") against Defendant Ethos Technologies, Inc. ("Ethos" or "Defendant"), to obtain damages, restitution, and injunctive relief for the Class, as defined below, from Defendant. Plaintiff makes the following allegations on information and belief, except as to her own actions, which are made on personal knowledge, the investigation of her counsel, and the facts that are a matter of public record.

NATURE OF CASE

1. This class action arises out of the recent targeted cyberattack and data breach ("Data Breach") on Ethos's network—through its third-party integrated service provider,

Guidewire—that resulted in unauthorized access to highly sensitive data.[1] As a result of the Data Breach, Class Members suffered ascertainable losses in the form of the benefit of their bargain, out-of-pocket expenses, the value of their time reasonably incurred to remedy or mitigate the effects of the attack, emotional distress, and the present risk of imminent harm caused by the compromise of their sensitive personal information.

2. The specific information compromised in the Data Breach includes personally identifiable information ("PII"), including full names and Social Security numbers.

3. Upon information and belief, prior to and through December 2022, Defendant obtained the PII of Plaintiff and Class Members and stored that PII, unencrypted, in an Internet-accessible environment on Ethos's network, in which unauthorized actors used an extraction tool to retrieve Social Security numbers from Ethos's third-party integrated service provider, Guidewire.

4. Plaintiff's and Class Members' PII—which was entrusted to Defendant, its officials, and agents—was compromised and unlawfully accessed due to the Data Breach.

5. Plaintiff brings this class action lawsuit on behalf of those similarly situated to address Defendant's inadequate safeguarding of her and Class Members' PII that Defendant collected and maintained, and for Defendant's failure to provide timely and adequate notice to Plaintiff and other Class Members that their PII had been subject to the unauthorized access of an unknown, unauthorized party.

6. Defendant maintained the PII in a negligent and/or reckless manner. In particular, the PII was maintained on Defendant's computer system and network in a condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the cyberattack and potential for

[1] https://dojmt.gov/wp-content/uploads/Consumer-notification-letter-21.pdf

improper disclosure of Plaintiff's and Class Members' PII was a known risk to Defendant, and thus Defendant was on notice that failing to take steps necessary to secure the PII from those risks left that property in a dangerous condition.

7. Upon information and belief, Defendant and its employees additionally failed to properly monitor the computer network, IT systems, and integrated service that housed Plaintiff's and Class Members' PII.

8. As a result of Defendant's negligent conduct, Plaintiff's and Class Members' identities are now at risk because the PII that Defendant collected and maintained is now in the hands of malicious cybercriminals. The risks to Plaintiff and Class Members will remain for their respective lifetimes.

9. Defendant failed to provide timely, accurate, and adequate notice to Plaintiff and Class Members. Plaintiff's and Class Members' knowledge about the PII that Defendant allowed to be compromised, as well as precisely what type of information was unencrypted and in the possession of unknown third parties, was unreasonably delayed by Defendant's failure to warn impacted persons immediately upon learning of the Data Breach.

10. In letters dated December 21, 2022, Ethos notified state Attorneys General and some Class Members about the widespread data breach that had occurred on Ethos's computer network and that Class Members' PII was accessed and acquired by malicious actors, using Guidewire's integrated insurance services (the "Notice").[2]

11. The Notice provided to the Montana Attorney General is as follows:

> **What Happened?** Ethos offers life insurance policies through an online application process. On December 8, 2022, we learned that unauthorized actors had launched a sophisticated and successful cyberattack against our website to access certain persons' SSNs. We immediately investigated the

[2] *Id.*

> incident and made a series of technical changes to our website to prevent further unauthorized access to SSNs. The vast majority of people affected by this incident were not existing Ethos customers.
>
> To access SSNs, the unauthorized actors entered information they had obtained about you from other sources—first and last name, date of birth, and address—into our online insurance application flow. This caused a third-party integrated service to return your SSN to the page source code on our website. Then, the unauthorized actors used specialized tools to extract SSNs from the page source code of our website. Importantly, these SSNs did not appear on the public-facing application page of the site. The incident spanned from approximately August 4, 2022 through December 9, 2022.
>
> **What Information Was Involved?** Social Security number.[3]

12. Ethos acknowledged that its investigation into the Data Breach determined there was unauthorized access to Plaintiff's and Class Members' Social Security numbers between August 4, 2022, and December 9, 2022. Ethos's investigation concluded, and it learned what information was available to the unauthorized actors, on December 8, 2022.

13. Ethos's Notice letter further admitted that the PII accessed included individuals' names and Social Security numbers.[4]

14. Armed with the PII accessed in the Data Breach, data thieves can commit a variety of crimes including opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' information to target other phishing and hacking intrusions using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

[3] *Id.*
[4] *Id.*

15. As a result of the Data Breach, Plaintiff and Class Members have been exposed to a present, heightened and imminent risk of fraud and identity theft. Plaintiff and Class Members must now closely monitor their financial accounts to guard against identity theft for the rest of their lives.

16. Plaintiff and Class Members may also incur out of pocket costs for purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

17. By her Complaint, Plaintiff seeks to remedy these harms on behalf of herself and all similarly situated individuals whose PII was accessed during the Data Breach.

18. Accordingly, Plaintiff brings claims on behalf of herself and the Class for: (i) negligence, (ii) invasion of privacy, (iii) unjust enrichment and (iv) violation of the California Unfair Competition Law. Through these claims, Plaintiff seeks, *inter alia*, damages and injunctive relief, including improvements to Defendant's data security systems and integrated services, future annual audits, and adequate credit monitoring services.

THE PARTIES

19. Plaintiff Josephine Dibisceglia is a natural person, resident, and a citizen of the State of Florida. Plaintiff Dibisceglia has no intention of moving to a different state in the immediate future. Plaintiff Dibisceglia is acting on her own behalf and on behalf of others similarly situated. Defendant obtained and continues to maintain Plaintiff Dibisceglia's PII and owes her a legal duty and obligation to protect that PII from unauthorized access and disclosure. Plaintiff Dibisceglia's PII was compromised and disclosed as a result of Defendant's inadequate data security, which resulted in the Data Breach.

20. Plaintiff received a notice letter from Ethos, dated December 21, 2022, stating that a data security incident occurred at Ethos and Plaintiff's PII was involved in the incident.

21. Defendant Ethos Technologies Inc. is a provider of insurance, specializing in life insurance. Defendant is headquartered at 75 Hawthorne Street, Suite 2000, San Francisco, California 94105.

JURISDICTION AND VENUE

22. This Court has original jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2) because at least one member of the putative Class, including Plaintiff, are citizens of a different state than Defendant, there are more than 100 putative class members, and the amount in controversy exceeds $5 million exclusive of interest and costs.

23. This Court has personal jurisdiction over Defendant because Defendant and/or their parents or affiliates are headquartered in this District and Defendant conducts substantial business in California and this District through its headquarters, offices, parents, and affiliates.

24. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because Defendant's principal places of business are in this District and a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District.

DIVISIONAL ASSIGNMENT

25. This Action is properly assigned to the San Francisco Division of this District pursuant to N.D. Cal. L.R. 3-2, because Ethos maintains its principal place of business in San Francisco, which is served by the San Francisco Division of this District.

DEFENDANT'S BUSINESS

26. Defendant Ethos is an insurance carrier, specializing in life insurance.

27. Upon information and belief, in the course of its day-to-day business operations, Defendant maintains the PII of customers, insurance applicants, and others, including but not limited to:

- Name, address, phone number and email address;
- Date of birth;
- Demographic information;
- Social Security number;
- Financial information;
- Information relating to individual medical history;
- Information concerning an individual's doctor, nurse, or other medical providers;
- Medication information,
- Health insurance information,
- Photo identification;
- Employment information, and;
- Other information that Defendant may deem necessary to provide care.

28. Additionally, Defendant may receive PII from other individuals and/or organizations that are part of a customers' "circle of care," such as referring physicians, customers' other doctors, customers' health plan(s), close friends, and/or family members.

29. Plaintiff and Class Members directly or indirectly entrusted Defendant with sensitive and confidential PII, which includes information that is static, does not change, and can be used to commit myriad financial crimes.

30. Upon information and belief, Defendant promised— due to the highly sensitive, confidential nature of the information it collects—to customers that Ethos would (among other

things) keep their PII private, comply with industry standards related to data security and PII; inform them of their legal duties and comply with all federal and state laws protecting PII; only use and release their PII for reasons that relate to medical care and treatment; and provide adequate notice if their PII is disclosed without authorization.

31. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' PII from unauthorized disclosure.

32. Plaintiff and the Class Members value their privacy and have taken reasonable steps to maintain the confidentiality of their PII.

33. Plaintiff and the Class Members relied on Defendant to implement and follow adequate data security policies and protocols, to keep their PII confidential and securely maintained, to use such PII solely for business purposes, and to prevent the unauthorized disclosures of their PII.

THE CYBERATTACK

34. On or around December 8, 2022, Ethos became aware of suspicious activity in its network environment and its website.

35. Defendant Ethos investigated the suspicious activity, and through its investigation, determined that its network was subject to a cyber-attack using the integrated service software on its website. Unauthorized actors exploited this integrated software to target, access, and acquire the PII without authorization.

36. The investigation determined that private information related to certain customers and other individuals on Ethos's website was accessed and taken by an unauthorized user between August 4, 2022, and December 9, 2022.

37. As Defendant admits, Plaintiff's and Class Members' PII was exfiltrated and stolen in the attack.

38. Upon information and belief, the unauthorized actors were able to access Ethos's insurance application flow on its website by entering certain consumer information that they had obtained through other sources. This simple maneuver prompted a return of the named consumers' Social Security numbers in the application. The PII was internet accessible, unencrypted, unprotected, and vulnerable to acquisition and/or exfiltration by the unauthorized actor.

39. It is likely the Data Breach was targeted at Defendant due to its status as an insurance related service provider that collects, creates, and maintains sensitive PII.

40. Upon information and belief, the cyberattack was expressly designed to gain access to private and confidential data of specific individuals, including (among other things) the PII of Plaintiff and the Class Members.

41. Ethos admitted that the stolen information included full names and Social Security Numbers.

42. While Ethos stated in the Notice letter that the unauthorized activity occurred and was discovered on December 8, 2022, Defendant did notify the specific persons or entities whose PII was acquired and exfiltrated until December 21, 2022—*over five months* after the Data Breach began on August 4, 2022.

43. Upon information and belief, and based on the type of cyberattack, it is plausible and likely that Plaintiff's PII was stolen in the Data Breach. Plaintiff further believes her PII was likely subsequently sold on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals.

44. Defendant had a duty to adopt reasonable measures to protect Plaintiff's and Class Members' PII from involuntary disclosure to third parties.

45. In response to the Data Breach, Ethos admits they worked with an "independent forensic investigation firm" to determine the nature and scope of the incident and purports to have taken steps to secure the systems.

46. Ethos admits additional security was required, but there is no indication whether these steps are adequate to protect Plaintiff's and Class Members' PII going forward.

47. Because of the Data Breach, data thieves were able to gain access to Defendant's supposedly secure systems for months (between August 4, 2022, and December 9, 2021) and were able to compromise, access, and acquire the protected PII of Plaintiff and Class Members.

48. Defendant had obligations created by contract, industry standards, common law, and their own promises and representations made to Plaintiff and Class Members to keep their PII confidential and to protect them from unauthorized access and disclosure.

49. Plaintiff and the Class Members reasonably relied (directly or indirectly) on this sophisticated party to keep their sensitive PII confidential; to maintain proper system security; to use this information for business purposes only; and to make only authorized disclosures of their PII.

50. Plaintiff's and Class Members' unencrypted, unredacted PII was compromised due to Defendant's negligent and/or careless acts and omissions, and due to the utter failure to

protect Class Members' PII. Criminal hackers obtained their PII because of its value in exploiting and stealing the identities of Plaintiff and Class Members. The risks to Plaintiff and Class Members will remain for their respective lifetimes.

The Data Breach was a Foreseeable Risk of which Defendant was on Notice

51. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the insurance industry and other industries holding significant amounts of PII preceding the date of the breach.

52. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[5] The 330 reported breaches reported in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.[6]

53. In light of recent high profile data breaches at other insurance partner and provider companies, Defendant knew or should have known that their electronic records and PII they maintained would be targeted by cybercriminals and ransomware attack groups.[7]

54. Moreover, Ethos knew or should have known that these attacks were common and foreseeable, as it discovered a separate and distinct but substantially similar data breach in January 2022, which also occurred for approximately several months.[8]

---

[5] *See* 2021 Data Breach Annual Report (ITRC, Jan. 2022) (available at https://notified.idtheftcenter.org/s/), at 6.
[6] *Id.*
[7] https://www.databreaches.net/rxamerica-and-accendo-insurance-notify-175000-medicare-beneficiaries-that-mailing-error-exposed-their-medication-name-date-of-birth-and-member-id/
[8] https://www.doj.nh.gov/consumer/security-breaches/documents/ethos-technologies-20220218.pdf

55. In light of recent high profile cybersecurity incidents at other insurance partners and provider companies, Ethos knew or should have known that their electronic records would be targeted by cybercriminals.[9]

56. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including Ethos.

Defendant Fails to Comply with FTC Guidelines

57. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

58. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand its network's vulnerabilities; and implement policies to correct any security problems.[10] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[11]

---

[9] https://www.databreaches.net/rxamerica-and-accendo-insurance-notify-175000-medicare-beneficiaries-that-mailing-error-exposed-their-medication-name-date-of-birth-and-member-id/

[10] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Jan. 19, 2022).

[11] *Id.*

59. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

60. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

61. These FTC enforcement actions include actions against insurance providers and partners like Defendant.

62. Defendant failed to properly implement basic data security practices.

63. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to customers and other impacted individuals' PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

64. Defendant was at all times fully aware of their obligation to protect the PII. Defendant was also aware of the significant repercussions that would result from their failure to do so.

Defendant Fails to Comply with Industry Standards

65. As shown above, experts studying cyber security routinely identify insurance providers and partners as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

66. Several best practices have been identified that at a minimum should be implemented by insurance providers, like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

67. Other best cybersecurity practices that are standard in the insurance industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

68. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

69. These foregoing frameworks are existing and applicable industry standards in the insurance industry, and Defendant failed to comply with these accepted standards, thereby opening the door to the cyber incident and causing the data breach.

DEFENDANT'S BREACH

70. Defendant breached its obligations to Plaintiff and Class Members and/or were otherwise negligent and reckless because Ethos failed to properly maintain and safeguard their computer systems and website's application flow. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately protect PII;

c. Failing to properly monitor their own data security systems for existing intrusions;

d. Failing to ensure that their vendors with access to their computer systems and data employed reasonable security procedures;

e. Failing to ensure the confidentiality and integrity of electronic PII it created, received, maintained, and/or transmitted;

f. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PII to allow access only to those persons or software programs that have been granted access rights;

g. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations;

h. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports;

i. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PII;

j. Failing to train all members of their workforces effectively on the policies and procedures regarding PII;

k. Failing to render the electronic PII it maintained unusable, unreadable, or indecipherable to unauthorized individuals;

l. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act;

m. Failing to adhere to industry standards for cybersecurity as discussed above; and,

n. Otherwise breaching their duties and obligations to protect Plaintiff's and Class Members' PII.

71. Defendant negligently and unlawfully failed to safeguard Plaintiff's and Class Members' PII by allowing cyberthieves to access Defendant's online insurance application flow, which provided unauthorized actors with unsecured and unencrypted PII.

72. Accordingly, as outlined below, Plaintiff and Class Members now face a present, increased risk of fraud and identity theft. In addition, Plaintiff and the Class Members lost the benefit of the bargain they made with Defendant.

Data Breaches Cause Disruption and Increased Risk of Fraud and Identity Theft

73. Cyberattacks and data breaches at insurance companies and insurance software companies, like Defendant, are especially problematic because they can negatively impact the overall daily lives of individuals affected by the attack.

74. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[12]

75. That is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal personally identifiable information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims, take over victims' identities in order to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

76. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent

[12] *See* U.S. Gov. Accounting Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (2007). Available at https://www.gao.gov/new.items/d07737.pdf.

charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[13]

77. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

78. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

79. Moreover, theft of PII is also gravely serious because PII is an extremely valuable property right.[14]

80. Its value is axiomatic, considering the value of "big data" in corporate America and the fact that the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that PII has considerable market value.

---

[13] *See IdentityTheft.gov*, Federal Trade Commission, https://www.identitytheft.gov/Steps (last visited Jan. 19, 2022).

[14] *See, e.g.,* John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

81. It must also be noted there may be a substantial time lag – measured in years -- between when harm occurs and when it is discovered, and also between when PII is stolen and when it is used.

82. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[15]

83. PII is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

84. There is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future.

85. Thus, Plaintiff and Class Members must vigilantly monitor their financial and medical accounts for many years to come.

86. PII can sell for as much as $363 per record according to the Infosec Institute.[16] PII is particularly valuable because criminals can use it to target victims with frauds and scams. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

---

[15] GAO Report, at p. 29.

[16] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/.

87. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[17] Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security Numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[18] Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

88. Moreover, it is not an easy task to change or cancel a stolen Social Security number.

89. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[19]

90. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit

[17] *Identity Theft and Your Social Security Number*, Social Security Administration (2018) at 1. Available at https://www.ssa.gov/pubs/EN-05-10064.pdf (Jan. 19, 2022).
[18] *Id* at 4.
[19] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft.

card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[20]

91. Because of the value of its collected and stored data, the insurance industry has experienced disproportionally higher numbers of data theft events than other industries.

92. For this reason, Defendant knew or should have known about these dangers and strengthened its data and email handling systems accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet Defendant failed to properly prepare for that risk.

Plaintiff's and Class Members' Damages

93. To date, Defendant has done nothing to provide Plaintiff and the Class Members with meaningful relief for the damages they have suffered as a result of the Data Breach.

94. Defendant has merely offered Plaintiff and Class Members complimentary fraud and identity monitoring services for up to two years, but this does nothing to compensate them for damages incurred, time spent dealing with the Data Breach, and future fraud and identity monitoring services (reasonable and necessary expenses) beyond the two years offered.

95. Plaintiff and Class Members have been damaged by the compromise of their PII in the Data Breach.

96. Plaintiff's and Class Members' full names and Social Security numbers were compromised in the Data Breach and are now in the hands of the cybercriminals who accessed Defendant's software maintaining PII. As Ethos admits, these impacted persons were specifically

[20] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.

targeted: the cybercriminals used their names, dates of birth and addresses to steal Plaintiff's and Class Members' Social Security numbers.

97. Since being notified of the Data Breach, Plaintiff has significant time dealing with the impact of the Data Breach—valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation.

98. Due to the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. This includes changing passwords, resecuring her own computer system, cancelling fraudulent credit and debit cards opened in her name, and monitoring her financial accounts for fraudulent activity.

99. Plaintiff's PII was compromised as a direct and proximate result of the Data Breach.

100. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been placed at a present, imminent, immediate, and continuing risk of harm from fraud and identity theft.

101. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been forced to expend time dealing with the effects of the Data Breach.

102. Plaintiff and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

103. Plaintiff and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their PII as potential fraudsters could use that information to more effectively target such schemes to Plaintiff and Class Members. Plaintiff has already experienced fraudulent conduct, as over seven thousand dollars in fraudulent

charges were placed upon her credit card and identity thieves have attempted to open new credit cards falsely under her name.

104. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

105. Plaintiff and Class Members also suffered a loss of value of their PII when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

106. Plaintiff and Class Members were also damaged via benefit-of-the-bargain damages. Plaintiff and Class Members overpaid for a service that was intended to be accompanied by adequate data security that complied with industry standards but was not. Part of the price Plaintiff and Class Members paid to Defendant was intended to be used by Defendant to fund adequate security of Defendant's systems and Plaintiff's and Class Members' PII. Thus, the Plaintiff and the Class Members did not get what they paid for and agreed to.

107. Plaintiff and Class Members have spent and will continue to spend significant amounts of time to monitor their financial accounts and sensitive information for misuse.

108. Plaintiff and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Reviewing and monitoring sensitive accounts and finding fraudulent insurance claims, loans, and/or government benefits claims;

b. Purchasing credit monitoring and identity theft prevention;

c. Spending time on the phone with or at financial institutions, healthcare providers, and/or government agencies to dispute unauthorized and fraudulent activity in their name;

d. Contacting financial institutions and closing or modifying financial accounts; and

e. Closely reviewing and monitoring Social Security Number, medical insurance accounts, bank accounts, and credit reports for unauthorized activity for years to come.

109. Moreover, Plaintiff and Class Members have an interest in ensuring that their PII, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of adequate security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing PII is not accessible online and that access to such data is password protected.

110. Further, as a result of Defendant's conduct, Plaintiff and Class Members are forced to live with the anxiety that their PII may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

111. As a direct and proximate result of Defendant's actions and inactions, Plaintiff and Class Members have suffered anxiety, emotional distress, and loss of privacy, and are at an increased risk of future harm.

Plaintiff Dibisceglia's Experience

112. Plaintiff Josephine Dibisceglia does not know how Defendant obtained her PII, and she had never heard of Defendant until she received the notice letter regarding the Data Breach in December 2022.

113. Plaintiff Dibisceglia is very careful about sharing her sensitive Private Information. Plaintiff Dibisceglia has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

114. Plaintiff Dibisceglia first learned of the Data Breach after receiving a data breach notification letter from Ethos, dated December 21, 2022, notifying her that Defendant suffered a data breach five months earlier and that her PII had been improperly accessed and/or obtained by unauthorized third parties while in possession of Defendant.

115. The data breach notification letter indicated that the PII involved in the Data Breach may have included Plaintiff Dibisceglia's full name and Social Security number.

116. As a result of the Data Breach, Plaintiff Dibisceglia made reasonable efforts to mitigate the impact of the Data Breach after receiving the data breach notification letter, including but not limited to researching the Data Breach; contacting her bank regarding fraudulent activity; contacting credit bureaus regarding fraudulent activity; and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud.

117. Plaintiff Dibisceglia experienced actual identify theft and fraud, including over seven thousand dollars of fraudulent charges being placed on her credit card as well as the identity thieves attempting to open additional credit cards falsely under her name. Plaintiff Dibisceglia has taken significant efforts to remedy her credit file as a result of the Data Breach.

118. Plaintiff Dibisceglia has spent several hours and will continue to spend valuable time for the remainder of her life, that she otherwise would have spent on other activities, including but not limited to work and/or recreation.

119. Plaintiff Dibisceglia suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value

of her PII, a form of property that Defendant maintained belonging to Plaintiff Dibisceglia; (b) violation of her privacy rights; (c) the theft of her PII; and (d) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

120. As a result of the Data Breach, Plaintiff Dibisceglia has also suffered emotional distress as a result of the release of her PII, which she believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using her PII for purposes of identity theft and fraud. Plaintiff Dibisceglia is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

121. As a result of the Data Breach, Plaintiff Dibisceglia anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

CLASS ACTION ALLEGATIONS

122. Plaintiff brings this action on behalf of herself and on behalf of all other persons similarly situated ("the Class").

123. Plaintiff proposes the following Class definitions, subject to amendment as appropriate:

> **All persons identified by Defendant (or their agents or affiliates) as being among those individuals impacted by the Data Breach, including all who were sent a notice of the Data Breach (the "Class").**

124. Excluded from the Class are Defendant's officers, directors, and employees; any entity in which Defendant have a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and members of their staff.

125. Plaintiff reserves the right to amend or modify the Class and/or Subclass definitions as this case progresses.

126. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, based on information and belief, the Class consists of thousands of individuals whose sensitive data was compromised in the Data Breach.

127. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' PII;

b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Defendant owed a duty to Class Members to safeguard their PII;

f. Whether Defendant breached its duty to Class Members to safeguard their PII;

g. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

h. Whether Defendant should have discovered the Data Breach sooner;

i. Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

j. Whether Defendant's conduct was negligent;

k. Whether Defendant breached implied contracts made with Plaintiff and Class Members;

l. Whether Defendant was unjustly enriched by unlawfully retaining a benefit conferred upon them by Plaintiff and Class Members;

m. Whether Defendant failed to provide notice of the Data Breach in a timely manner; and,

n. Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, treble damages, and/or injunctive relief.

128. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's information, like that of every other Class Member, was compromised in the Data Breach.

129. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel are competent and experienced in litigating class actions.

130. Predominance. Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members' data was stored on the same computer system and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any

individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

131. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

132. Defendant has acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

133. Likewise, particular issues under Rule 42(d)(l) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant failed to timely notify the public of the Data Breach;

b. Whether Defendant owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their PII;

c. Whether Defendant's security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;

d. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;

e. Whether Defendant failed to take commercially reasonable steps to safeguard consumer PII; and,

f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

134. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendant.

CAUSES OF ACTION

FIRST COUNT
Negligence
(On Behalf of Plaintiff and the Class)

135. Plaintiff re-alleges and incorporates by reference by reference herein all of the allegations contained in the preceding paragraphs.

136. Plaintiff and the Class entrusted Defendant with their PII on the premise and with the understanding that Defendant would safeguard their information, use their PII for business purposes only, and/or not disclose their PII to unauthorized third parties.

137. Defendant had full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and the Class could and would suffer if the PII were wrongfully disclosed.

138. By collecting and storing this data on Ethos' computer system and network, and sharing it and using it for commercial gain, Defendant owed a duty of care to use reasonable means to secure and safeguard their computer system—and Class Members' PII held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which it could detect a breach of their security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

139. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that their systems and networks, and the personnel responsible for them, adequately protected the PII.

140. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and the individuals who entrusted them with PII, which is recognized by laws and regulations, as well as common law. Defendant was in a superior position to ensure that their systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

141. Defendant's duty to use reasonable security measures required Defendant to reasonably protect confidential data from any intentional or unintentional use or disclosure.

142. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

143. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant are bound by industry standards to protect confidential PII.

144. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' PII. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' PII;

b. Failing to adequately monitor the security of their networks and systems;

d. Failing to have in place mitigation policies and procedures;

e. Allowing unauthorized access to Class Members' PII;

f. Failing to detect in a timely manner that Class Members' PII had been compromised; and,

g. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

145. Defendant owed to Plaintiff and Class Members a duty to notify them within a reasonable timeframe of any breach to the security of their PII. Defendant also owed a duty to timely and accurately disclose to Plaintiff and Class Members the scope, nature, and occurrence of the data breach. This duty is required and necessary for Plaintiff and Class Members to take appropriate measures to protect their PII, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the data breach.

146. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.,* (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

147. Defendant breached its duties to Plaintiff and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PII.

148. Defendant owed these duties to Plaintiff and Class Members because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security protocols. Defendant actively sought and obtained Plaintiff's and Class Members' PII.

149. The risk that unauthorized persons would attempt to gain access to the PII and misuse it was foreseeable. Given that Defendant held vast amounts of PII, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the PII—whether by malware or otherwise.

150. PII is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII of Plaintiff and Class Members and the importance of exercising reasonable care in handling it.

151. Defendant breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the PII of Plaintiff and Class Members—which actually and proximately caused the Data Breach and injured Plaintiff and Class Members.

152. Defendant further breached its duties by failing to provide reasonably timely notice of the data breach to Plaintiff and Class Members, which actually and proximately caused and exacerbated the harm from the data breach and Plaintiff and Class Members' injuries-in-fact. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiff and Class Members have suffered and/or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

153. Defendant's breach of its common-law duties to exercise reasonable care and their failures and negligence actually and proximately caused Plaintiff and Class Members actual, tangible, injury-in-fact and damages, including, without limitation, fraudulent credit card charges, financial accounts being opened falsely in their name, the theft of their PII by criminals, improper disclosure of their PII, lost benefit of their bargain, lost value of their PII, and lost time and money incurred to mitigate and remediate the effects of the data breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

SECOND COUNT
Invasion of Privacy
(On behalf of the Plaintiff and the Class)

154. Plaintiff re-alleges and incorporates by reference by reference herein all of the allegations contained in the preceding paragraphs and brings this claim under the common law and Art. I § I of the California Constitution.

155. Plaintiff and Class Members had a legitimate expectation of privacy regarding their PII and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

156. Defendant owed a duty to Plaintiff and Class Member to keep their PII confidential.

157. The unauthorized disclosure and/or acquisition (*i.e.,* theft) by a third party of Plaintiff's and Class Members' PII is highly offensive to a reasonable person.

158. Defendant's reckless and negligent failure to protect Plaintiff's and Class Members' PII constitutes an intentional interference with Plaintiff's and the Class Members' interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

159. Defendant's failure to protect Plaintiff's and Class Members' PII acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

160. Defendant knowingly did not notify Plaintiff and Class Members in a timely fashion about the Data Breach.

161. Because Defendant failed to properly safeguard Plaintiff's and Class Members' PII, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiff and the Class.

162. As a proximate result of Defendant's acts and omissions, the private and sensitive PII of Plaintiff and the Class Members was stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiff and the Class to suffer damages.

163. Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class since their PII is still maintained by Defendant with their inadequate cybersecurity system and policies.

164. Plaintiff and Class Members have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendant's inability to safeguard the PII of Plaintiff and the Class.

165. Plaintiff, on behalf of herself and Class Members, seeks injunctive relief to enjoin Defendant from further intruding into the privacy and confidentiality of Plaintiff's and Class Members' PII.

166. Plaintiff, on behalf of herself and Class Members, seeks compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest, and costs.

THIRD COUNT
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

167. Plaintiff re-alleges and incorporates by reference by reference herein all of the allegations contained in the preceding paragraphs.

168. Upon information and belief, Defendant funds its data security measures entirely from their general revenue, including payments made by or on behalf of Plaintiff and the Class Members.

169. As such, a portion of the payments made by or on behalf of Plaintiff and the Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

170. Plaintiff and Class Members conferred a monetary benefit upon Defendant. Specifically, they purchased goods and services from Defendant and/or their agents and in so

doing provided Defendant with their PII. In exchange, Plaintiff and Class Members should have received from Defendant the goods and services that were the subject of the transaction and have their PII protected with adequate data security.

171. Plaintiff and Class Members conferred a monetary benefit on Defendant, by paying Defendant as part of Defendant rendering insurance related services, a portion of which was to have been used for data security measures to secure Plaintiff's and Class Members' PII, and by providing Defendant with their valuable PII.

172. Defendant knew that Plaintiff and Class Members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the PII of Plaintiff and Class Members for business purposes.

173. Defendant was enriched by saving the costs they reasonably should have expended on data security measures to secure Plaintiff's and Class Members' PII. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to avoid the data security obligations at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

174. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

175. Defendant acquired the monetary benefit and PII through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

176. If Plaintiff and Class Members knew that Defendant had not secured their PII, they would not have agreed to provide their PII to Defendant.

177. Plaintiff and Class Members have no adequate remedy at law.

178. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury including, without limitation, fraudulent credit card charges, financial accounts being opened falsely in their name, the theft of their PII by criminals, improper disclosure of their PII, lost benefit of their bargain, lost value of their PII, and lost time and money incurred to mitigate and remediate the effects of the data breach that resulted from and were caused by Defendant's misconduct, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

179. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

180. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff and Class Members overpaid for Defendant's services.

FOURTH COUNT
Violation of the California Unfair Competition Law
[Cal. Bus. & Prof. Code § 17200, *et seq.* – Unlawful Business Practices]
(On Behalf of Plaintiff and the Class)

181. Plaintiff re-alleges and incorporates by reference all prior paragraphs as if fully set forth herein.

182. Ethos violated Cal. Bus. and Prof. Code § 17200, *et seq.,* by engaging in unlawful, unfair or fraudulent business acts and practices and unfair, deceptive, untrue or misleading

advertising that constitute acts of "unfair competition" as defined in Cal. Bus. Prof. Code § 17200 with respect to the services provided to the Class.

183. Ethos engaged in unlawful acts and practices with respect to the services by establishing the sub-standard security practices and procedures described herein; by soliciting and collecting Plaintiff's and Class Members' PII with knowledge that the information would not be adequately protected; and by storing Plaintiff's and Class Members' PII in an unsecure electronic environment in violation of California's data breach statute, Cal. Civ. Code § 1798.81.5, which requires Ethos to take reasonable methods for safeguarding the PII of Plaintiff and the Class Members.

184. In addition, Ethos engaged in unlawful acts and practices by failing to disclose the Data Breach in a timely and accurate manner, contrary to the duties imposed by Cal. Civ. Code § 1798.82.

185. As a direct and proximate result of Ethos's unlawful practices and acts, Plaintiff and Class Members were injured and lost money or property, including but not limited to the price received by Ethos for the products and services, the loss of Plaintiff's and Class Members' legally protected interest in the confidentiality and privacy of their PII, nominal damages, and additional losses as described herein.

186. Ethos knew or should have known that its computer systems and data security practices were inadequate to safeguard Plaintiff's and Class Members' PII and that the risk of a data breach or theft was highly likely. Ethos's actions in engaging in the above-named unlawful practices and acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiff and Class Members.

187. Plaintiff, on behalf of the Class, seeks relief under Cal. Bus. & Prof. Code § 17200, *et seq.,* including, but not limited to, restitution to Plaintiff and Class Members of money or property that Ethos may have acquired by means of its unlawful, and unfair business practices, restitutionary disgorgement of all profits accruing to Ethos because of its unlawful and unfair business practices, declaratory relief, attorneys' fees and costs (pursuant to Cal. Code Civ. Proc. § 1021.5), and injunctive or other equitable relief.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and Class Members, requests judgment against Defendant and that the Court grant the following:

A. For an Order certifying the Class, and appointing Plaintiff and her Counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII of Plaintiff and Class Members;

C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendant to delete, destroy, and purge the personal identifying

information of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Defendant to provide out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII for Plaintiff's and Class Members' respective lifetimes;

v. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiff and Class Members;

vi. prohibiting Defendant from maintaining the PII of Plaintiff and Class Members on a cloud-based database;

vii. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

viii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

ix. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

x. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised,

hackers cannot gain access to other portions of Defendant's systems;

xi. requiring Defendant to conduct regular database scanning and securing checks;

xii. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

xiii. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiv. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xvi. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvii. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of damages, including actual, nominal, statutory, consequential, and punitive damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff hereby demands that this matter be tried before a jury.

Dated: January 11, 2023

Respectfully Submitted,

/s/ *John Nelson*

John J. Nelson (SBN 317598)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN PLLC
401 W Broadway, Suite 1760
San Diego, CA 92101
Tel: (858) 209-6941
jnelson@milberg.com